本レポートの要点

第4四半期に、境界ベースのマルウェアの数は増加しましたが、ネットワーク攻撃は減少しました。

ネットワークマルウェアの検知数が全体として減少しました。マルウェア検知の未加工の数は80%近く増加し、ウォッチガードの挙動検知サービスであるAPT Blockerがブロックした高度な回避型の脅威は37%増加しました。

第3四半期とは異なり、第4四半期はネットワーク攻撃が減少して、約10%減となりました。しかしながら、ネットワーク攻撃の多様さの指標である一意の検知数は、この四半期に約16%増加しました。リモートでコード実行を可能にする恐れのある、Microsoft Exchangeの重大な脆弱性であるProxyLogonは、順位を1つ下げたものの、上位のネットワーク攻撃に引き続き入り、件数も増加しました。2020年あるいは2021年にパッチが適用され、この重大な脆弱性が修正されていることを願うばかりです。

ネットワークベースのマルウェア検知と比較すると、エンドポイントにおけるマルウェア検知数は前四半期比で継続して減少しています。古い脅威が今も10位までの上位に入り続けていますが、ウォッチガード製品でそれらの古い脅威はブロックされます。不正スクリプトがマルウェアペイロードを被害者のコンピュータに配布する最も一般的な方法であることに変わりありませんが、Windowsベースのファイルは引き続き、重要な第2の攻撃ベクトルとなっています。

この四半期の主な調査結果を箇条書きにまとめて以下に紹介します。

- **ネットワークベースのマルウェアの合計検知数が80%近く増加**し、APT Blockerサービスによるマルウェア検知が37%増となったことは、高度な回避型のマルウェアが増加し続けていることを示しています。これは、機械学習によって検知されたマルウェアが196%も増加したことからも明らかです。
- それぞれのネットワークマルウェア検知サービスにおける「Fireboxあたりの」マルウェア検知の結果は以下のとおりです。
  - **Fireboxあたりの平均マルウェア検知数の合計：2,416**（80%弱の増加）
  - **FireboxあたりのGAVによる平均マルウェア検知数：520**（2.6%増）
  - **FireboxあたりのIAVによる平均マルウェア検知数：1,404**（196%増）
  - **FireboxあたりのAPT Blockerによる平均マルウェア検知数：492**（37%弱の増加）
- テレメトリの共有に同意していただいたすべてのFireboxですべてのマルウェア検知サービスが有効になっていた場合、**2023年第4四半期のマルウェア検知は193,280,000**だったと推定されます。注意点として、この数はデータの共有に同意していただいたFireboxのみのものであり、世界中のすべてのアクティブなFireboxが含まれていた場合、この数は大幅に大きくなるはずです。
- **暗号化（TLS）に隠れるマルウェアの割合が、第4四半期に55%に増加しました。**過去最高ではなかったものの、HTTPS Webトラフィックを復号しなければ、ネットワーク経由のマルウェアの半数以上を見逃すことになることを示しています。
- **第4四半期に、ゼロデイマルウェアがマルウェア全体の60%を占めました。**ゼロデイマルウェアとは、シグネチャベースの防御を回避し、機械学習によるマルウェアモデルや挙動分析によってのみ検知されるマルウェアのことです。さらには、TLS経由で検知されたゼロデイマルウェアが10%増加して60%になりました。
- **5位までのマルウェアのうちの2つの亜種が、DarkGateネットワークにリダイレクトしていました。**最も広範囲で観察された5位までのマルウェアに、JS.Agent.USFとTrojan.GenericKD.67408266が入りましたが、どちらの亜種も、ユーザを不正リンクにリダイレクトし、どちらのマルウェアローダも、被害者のコンピュータにDarkGateマルウェアをロードしようとします。
- **ネットワーク攻撃が前四半期比で16%減少しました。**しかしながら、攻撃者が使用するネットワークエクスプロイトの多様さの指標である一意のネットワーク攻撃が16%近く増加しました。
- **ProxyLogonは、この四半期に悪用された攻撃の上位に引き続き入りました。**これは、Microsoft Exchange Serverのリモートコード実行の脆弱性で、かなり前にパッチが適用されているはずです。10位までの順位は下げて2位になったものの、件数は少し増加したようです。
- **最も広範囲で観察された5位までのネットワーク脆弱性のうちの4つがMicrosoft関連のソフトウェアを標的にし、**これには、ProxyLogon、ProxyShell、ProxyNotShellなどの名前の脆弱性が含まれます。
- **ウォッチガードのエンドポイント保護製品は、10万台のマシンあたり108の一意のマルウェア亜種をブロックし、**第3四半期に引き続き減少しました。端的に言えば、エンドポイントを攻撃するマルウェアが減少傾向にあるようです。ただし、ネットワークベースのマルウェアの検知が増加していることから、これは当然のことと言えます。境界でマルウェアが検知されれば、エンドポイントが攻撃されることはありません。
- **エンドポイントランサムウェア攻撃が19.7%近く減少しました。**ランサムウェアが今後もマルウェアペイロードの首位に立つ可能性が高いものの、最近はほとんど変動しない状態が続いています。おそらくは、捜査機関が多くのランサムウェアグループを解体したことが、この減少につながっています。残念ながら、これらの亜種は解体されたものの、いずれは復活することが予想されます。

- **サイバー攻撃のコモディティ化が進み、Victim-as-a-Service（被害者がサービスとして提供される）ようになりつつあります。**GluptebaとGuLoaderは、第4四半期に最も広範囲で観察されたエンドポイントマルウェアの10位までに再び入り、第4四半期に分析された、最も一般的な亜種の2つとして返り咲きました。Gluptebaは、世界規模で被害者を標的にしているという点でも、特に注目に値する、強力で高度なマルウェアです。Gruptebaは、追加マルウェアのダウンロード、ボットネットとしての偽装、機密情報の窃取、驚異的なステルス性を備えた暗号通貨のマイニングなどのさまざまな機能を提供するMaaS（Malware-as-a-Service）です。
- **不正スクリプトは今なお最も一般的なマルウェアの感染ベクトルです。**悪意のPowerShellやJavaScriptに十分に注意する必要があります。
- **不正SharePointのサブドメインが、不正リンクの首位に返り咲きしました。**侵害されたWordPressサイトに不正リンクや不正ドメインが置かれる例も増加しています。

以上は、この四半期のレポートで紹介するハイライトの一部に過ぎません。本レポートでは、多くの防衛戦略やセキュリティのヒントを始めとする、さらに興味深い詳しいデータや追加情報を紹介します。四半期ごとのサイバー脅威の「地図」がお読みいただく方にとって役に立つものであることを願っています。